ERNEST J. ISTOOK, JR.
5TH DISTRICT, OKLAHOMA

COMMITTEE:
APPROPRIATIONS
SUBCOMMITTEES:
CHAIRMAN,
DISTRICT OF COLUMBIA
LABOR, HHS, AND EDUCATION
DEFENSE

ASSISTANT MAJORITY WHIP

DOCKET FILE COPY ORIGINAL

Congress of the United States

House of Representatives

Washington, DC 20515–3605

2404 RAYBURN BUILDING
WASHINGTON, DC 20515–3605
(202) 225–2132
FAX (202) 226–1463

DISTRICT OFFICES:
5400 N. GRAND BOULEVARD
SUITE 505
OKLAHOMA CITY, OK 73112
(405) 942–3636
FAX (405) 942–3792

117 W. 5TH STREET
BARTLESVILLE, OK 74003
(918) 336–5546
FAX (918) 336–5740

5TH & GRAND
PONCA CITY, OK 74601
(580) 762–6778
FAX (580) 762–7049

istook@mail.house.gov

February 15, 2001

Magalie Roman Salas
Office of the Secretary
Federal Communications Commission
445 12th St SW
Washington, D.C. 20554

Sheryl Todd
Accounting Policy Division
Common Carrier Bureau
Federal Communications Commission
445 Twelfth St SW, Room 5-B540
Washington, D.C. 20554

Subject: Public Comment on CC Docket No. 96-45, The Children's Internet Protection Act (CHIP)

Dear Madam Secretary:

As a major author of the Children's Internet Protection Act, I am commenting on the notice of proposed rulemaking, CC Docket No. 96-45.

Before becoming a Member of Congress, I served both as a member and later Chairman of a major metropolitan library board. I have a great interest in effectively protecting children, yet I am sensitive to the concerns of librarians.

Congress is intent on fashioning solutions to maximize protection for children on the Internet. In 1998, Congress tried to protect children from obscenity with the "Child Online Protection Act." That legislation required adult identification before admission to a site. The courts blocked this since some adults may not have appropriate identification and might be denied access.

Therefore, the new legislation is tightly focused and targeted—specific to minors and to federally-funded access. This effort actually started in 1998. Since then the Labor-HHS-Education Appropriations subcommittee persistently adopted a form of this new law. This provision was supported by every member of the subcommittee, both Democrat and Republican. The roll call vote was unanimous. Yet final passage was blocked by various forces until this year.

This year consensus was finally reached between House and Senate members. Senator McCain and Representatives Goodling, Pickering, and Istook coordinated the ultimate language .

The legislative summary is as follows:

- A school or library *which receives Federal funds from Title III, Library appropriations or the E-Rate for the purchase of computers, equipment to connect ot the Internet, or Internet connections* will install Internet Filters on equipment to protect adults and minors.

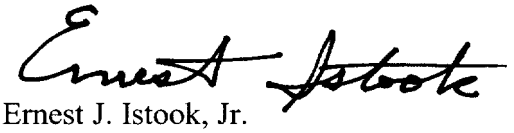
- Filters will block Obscenity and Child Pornography for all users, and during use by minors, computers will block material deemed harmful to minors or inappropriate for minors.

- Since filters may not be perfect, a bypass is permitted to conduct bonafide research or access constitutionally protected speech.

If the filtering software is not installed, the school or library involved would have funds withheld for further payments toward computers and computer-related services, until they comply with the law.

As one of the principal authors of the legislation, I hope you will give my comments suitable weight as you move forward with this rulemaking.

Very truly yours,



Ernest J. Istook, Jr.
Member of Congress

My compliments to the FCC for its prompt notice of proposed rule-making in response to the quick deadlines required under the Act. I agree with the Commission's general thrust, that regulatory provisions must ensure compliance without being burdensome to schools and libraries. Within that context, I offer the following constructive recommendations.

I. Public Disclosure

The FCC proposes that certification be achieved by adding new sections to FCC forms that would ask schools and libraries to certify whether they are in compliance with the Act, or that the provisions of the Act do not apply. This process can be properly characterized as a self-certification approach. While helpful, self-certification alone is insufficient to ensure that complete compliance is in fact occurring. A more open and public process should be required to avoid inadvertent non-compliance with the Act. Some schools and libraries may not be familiar with all of the requirements of the law and may believe they are in compliance when they are actually only in partial compliance. Others may inadvertently check the certification box on the form yet not be in compliance.

More specificity should be required -- with simple public disclosure as a safeguard. Public disclosure of Internet safety information is crucial to ensure full compliance. Library patrons and the parents of school children have both a right and a vested interest in knowing whether their local schools and libraries are in compliance.

To expand self-certification, schools and libraries should be required to publicly post the following information (including on their websites and public bulletin boards):

Written certification of compliance with the Act expressly specifying that they followed,

- The key requirements of the Act -- i.e., holding a public hearing, establishing an Internet safety policy, installing technology protection measures on computers, and using these measures to filter the categories of content enumerated under the Act;
- The text of the written Internet safety policy adopted;
- The name of the vendor of the technology protection measure chosen;
- Instructions on how the public may register comments or complaints with the FCC's Consumer Information Bureau; and,
- Instructions on how the public may register comments or complaints with the school or library.

Public disclosure serves two valuable purposes. First, it fulfills a core purpose of the Act – to inform the parents of school children and library patrons about the measures taken to protect against access to illegal or objectionable content. (Since a public hearing is required, its

participants will want to know what policy was eventually adopted. Parents who do not participate will also want to know.)

Second, public disclosure assures that the public will assist in monitoring compliance. Once parents or patrons know the requirements of the Act are, they can call attention to the non-compliance.

II. Complaint Procedure for the FCC and for Schools and Libraries

Procedures for registering public comments and complaints should be one of the publicly posted items in schools and libraries. Schools and libraries should be encouraged to keep written records of all comments, including the web addresses of sites that were under or over blocked. This permits invaluable exchange of information that will aid improvements of the technology (without disclosing the users' identities). There is ample precedent for providing complaint procedures to ensure compliance with other federal laws. The FDA, for example, has procedures to report adverse reactions to drugs.

A system for Internet user feedback will ensure that the policies adopted and the technological protection measures chosen actually work. Schools and libraries may evaluate the effectiveness of their policies and protection measures by reviewing the written record of comments received. Over time, decision makers may find that certain Internet safety policies are either under- or over-protective. Policies and measures can then be adjusted and improved, as needed.

As with FDA adverse event reports, copies of comments received should be made publicly available (with user's personal information redacted) so that the public can make its own judgement about how effective the policies and measures are in practice.

III. Effectiveness as an Element of Compliance

Compliance in the second and subsequent years should be measured differently than compliance in the first year. First year compliance amounts to getting the systems in place, e.g. a hearing, a policy, and a protection measure installed. In subsequent years, schools and libraries should also be required to self-certify on the appropriate FCC forms their assessment of how and why the policies and protection measures are actually working. The standard should be whether they are substantially effective in filtering the categories of content enumerated in the Act. If they are not, then the school or library should adjust its policy or choose a different technology protection measure, (such as changing the software package), so that it could remain eligible for federal funds. The purpose behind the Act will be subverted if certification of effectiveness is not required in the second and subsequent years.

IV. Certification by Each School and Library

The FCC seeks comment on whether certification should be submitted by school and library systems or by individual schools or libraries. Certification should involve each individual school and library, possibly by itemization within a group certification. Large systems in

particular, may have most but not all, of their schools or libraries in compliance by the deadline. Access to federal funds to other institutions in a system should not be jeopardized by the inaction of a few schools or libraries. Conversely, federal funds should not flow to a school or library that is not in compliance with the Act. The system should affirmatively certify that federal funds will not flow to those institutions.

V. Tracking Noncompliance

The FCC seeks comment on the noncompliance provisions of the Act. The notice of proposed rule making notes the provisions of the Act dealing with "willful" noncompliance. It is noted that the Act also includes provisions, § 3601 (a)(4) and § 1712 (a)(5), that address "failing to substantially comply." In either case, it is assumed that the Secretary of Education and The Director of the Institute of Museum and Library Services will faithfully follow the sanction procedures outlined in these sections. In addition, the FCC should ask these agencies to develop an annual summary of compliance activities, listing the instances of noncompliance that were brought to their attention and the actions taken. These summaries should be made publicly available.

VI. Comprehensive Language of Certification

The FCC seeks comments on the proposed language of self-certification. The FCC proposes generic language, that the recipient complies with "all the relevant provisions of the Children's Internet Protection Act." It must be stressed to recipients that certification is not a casual matter -- thus the certification should involve specifics. For example, a recipient may think that establishing an Internet safety policy without also installing technological protection measures may be sufficient. This problem is easily solved by substituting the phrase "all the relevant provisions" with more expansive language such as "the provisions of the Children's Internet Protection Act, which include requirements for a public hearing, the adoption of an Internet safety policy, and the installation of technology protection measures."

VII. Certification Timing Requirements

The FCC seeks comments on the timing requirements for certification and notes that while the Act establishes a time frame for enforcement, it does not establish a similar time frame for compliance with the Internet safety policy. The Commission asks whether the timing requirements for certification should also apply to compliance. Yes -- the timing requirements for certification should also apply to compliance. This was assumed by the authors of this legislation to be covered clearly in the legislation, without needing additional wording.

VIII. Concerns about what "access" to the Internet means

Discussions with the American Library Association have also shown a possible misinterpretation of the intent of the legislation. Because of dynamic technology, schools and libraries also use closed computer systems that do not have access to the "World-Wide Web", yet are, in fact, connected through the Internet. They use the Internet as the network portal or

pipeline to connect computers, yet the only thing accessible on those computers may be a card catalog -- or a professional periodicals database, for example.

It is my opinion that these computers do not require filtering, if they cannot be used to access Internet material outside of that specifically included in the closed system. (Naturally, if items within the closed system violate the CIPA law, or if the computer is ever set up for World-Wide Web access, it would have to be filtered to be in compliance with the law.) I believe this problem should be clarified in the FCC regulation.

IX. The FCC's Clarification of what Obscenity, Child Pornography or Harmful to Minors means

Because of their breadth, the terms obscenity, child pornography, or harmful to minors are chiefly defined by court rulings. What do these materials mean in lay-language? I believe the FCC will find the following attached excerpt from *Kids Online: Protecting Your Children in Cyberspace,* legally accurate, and I believe it should be incorporated into the regulation and public information to help citizens understand what their children are being protected from.

Definitions of Obscenity, Child Pornography and Material Harmful to Minors

(Mr. Istook's Note: References in this excerpt that refer to other media, such as movies or television, should be enlarged to include computers as well.)

Excerpted in part from Appendix D: *Pornography on the Internet, Kids Online: Protecting Your Children In Cyberspace* by Donna Rice Hughes (Revell, Fleming H., Baker Book House, September 1998)

Definitions

child pornography—Material that visually depicts children (real as well as computer-generated) under the age of eighteen engaged in actual or simulated sexual activity, including lewd exhibition of the genitals. Child pornography laws were recently amended to include computerized images or altered (morphed) pictures of children and counterfeit or synthetic images generated by computer that appear to be of real minors or that were marketed or represented to be real child pornography.

harmful to minors—Material harmful to minors represents nudity or sex that has prurient appeal for minors, is offensive and unsuitable for minors, and lacks serious value for minors. This material, also known as soft-core pornography, is legal for adults, but it is illegal to knowingly sell this material to children under the age of eighteen. There are harmful to minors laws in every state.

indecency—Includes messages or pictures on telephone, radio, or broadcast TV that are patently offensive descriptions or depictions of sexual or excretory organs or activities. This is also known as sexual nudity and "dirty words." There is currently no federal indecency statute that applies to the Internet.

obscenity—Graphic material that focuses on sex and/or sexual violence and is, therefore, prurient, patently offensive, and lacking in serious value. It is often referred to as hard-core pornography and includes close-ups of graphic sex acts and deviant activities, such as penetration, group sex, bestiality, torture, incest, and excretory functions. There are federal and state obscenity laws that forbid transmitting obscenity on the Internet but they have not been vigorously enforced.

(Production, transmission, and distribution of this material are felonies, yet possession of obscenity in one's home is not a crime. However, use of a phone line or online service to transmit obscenity is a federal crime under current law. Therefore, it is a felony to either *upload* (transmit from your personal computer to the Internet) or *download* (copy from the Internet onto your personal computer) Internet obscenity.

Because of the subjective nature of current obscenity law, content prosecutable as obscenity is widely available on the Internet, not because it is legal, but because it must be treated as "constitutionally protected" until it has received due process and has been proven illegal in a court of law. Consequently, children have access to content that could be prosecuted as obscenity, such as pictures of women engaged in sexual acts with animals (bestiality).)

Legal Definitions

child pornography—An unprotected visual depiction of a minor child (federal age is under eighteen) engaged in actual or simulated sexual conduct, including a lewd or lascivious exhibition of the genitals. *See New York v Ferber*, 458 U.S. 747 (1982), *Osborne v Ohio*, 495 U.S. 103 (1990), *U.S. v X-Citement Video, Inc.*, 115 S. Ct. 464 (1994). *See also U.S. v Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987), *U.S. v Knox*, 32 F.3d 733 (3rd Cir. 1994), *cert. denied*, 115 S. Ct. 897 (1995). Note: In 1996, 18 U.S.C. § 2252A was enacted and § 2256 was amended to include "child pornography" that consists of a visual depiction that "is or appears to be" of an actual minor engaging in sexually explicit conduct. *See Free Speech Coalition v Reno*, No. C-97-0281 SC, *judgment for defendants*, Aug. 12, 1997, *unpublished*, 1997 WL 487758 (N.D.Cal 1997).

obscenity (adult)—Not protected by the First Amendment. The "*Miller* Test" applies to actual or simulated sexual materials and lewd genital exhibitions. *See Miller v California,* 413 U.S. 15, at 24-25 (1973); *Smith v United States,* 431 U.S. 291, at 300-02, 309 (1977); *Pope v Illinois,* 481 U.S. 497, at 500-01 (1987), providing the three-pronged constitutional criteria for federal and state laws and court adjudications:

1. whether the average person, applying contemporary adult community standards, would find that the material, taken as a whole, appeals to a prurient interest in sex (i.e., an erotic, lascivious, abnormal, unhealthy, degrading, shameful, or morbid interest in nudity, sex, or excretion); and
2. whether the average person, applying contemporary adult community standards, would find that the work depicts or describes, in a patently offensive way, sexual conduct (i.e., ultimate sex acts, normal or perverted, actual or simulated; masturbation; excretory functions; lewd exhibition of the genitals; or sadomasochistic sexual abuse); and
3. whether a reasonable person would find that the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

material harmful to minors—Known as "variable obscenity" or the "*Millerized Ginsberg* Test." *See Ginsberg v New York*, 390 U.S. 629 (1968); and *Miller, Smith, Pope, supra.* It is illegal to sell, exhibit, or display "harmful" ("soft-core") pornography to minor children, even if the material is not obscene or illegal for adults. *See also Com. v Am. Booksellers Ass'n*, 372 S.E.2d 618 (Va. 1988), *followed, American Booksellers Ass'n v Com. of Va.*, 882 F.2d 125 (4th Cir. 1989), *Crawford v Lungren*, 96 F.3d 380 (9th Cir. 1996), *cert. denied*, 117 S. Ct. 1249 (1997). "Harmful to minors" means any written, visual, or audio matter of any kind that:

1. the average person, applying contemporary community standards, would find, taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion, and
2. the average person, applying contemporary community standards, would find depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, ultimate sexual acts, normal or perverted, actual or simulated; sadomasochistic sexual acts or abuse; or lewd exhibitions of the genitals, pubic area, buttocks, or post-pubertal female breast, and
3. a reasonable person would find, taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

broadcast indecency—*See FCC v Pacifica Foundation,* 438 U.S. 726 (1978). The FCC defines broadcast indecency as language or material that, *"in context, depicts or describes in terms patently offensive as measured by contemporary community standards for the broadcast medium, sexual or excretory activities or organs." Action For Children's Television v FCC,* 11 F.3d 170, 172 (D.C. Cir. 1993). Enforced by FCC from 6 AM–10 PM. *Action For Children's Television, et al. v F.C.C.,* 58 F.3d 654 (D.C. Cir. 1995), *cert. denied,* 116 S. Ct. 701 (1996).

dial-a-porn—*"The description or depiction of sexual or excretory activities or organs in a patently offensive manner as measured by contemporary community standards for the telephone medium."* Requires: a written request from an adult; or a credit card number; or an adult identification PIN code before transmission. *See Sable Communications of California, Inc. v FCC,* 492 U.S. 115, 126, 128-30 (1989); *Information Providers' Coalition v FCC,* 928 F.2d 866, 872 (9th Cir. 1991); *Dial Information Services Corporation of New York v Thornburgh,* 938 F.2d 1535 (2nd Cir. 1991), *cert. denied,* 502 U.S. 1072 (1992).

cable indecency—Cable operators may refuse to carry indecent leased access programming that the operator reasonably believes *"describes or depicts sexual or excretory activities or organs in a patently offensive manner as measured by contemporary community standards for the cable medium."* Cable operators who choose to carry indecent programming on leased access channels are not required to place such programs on a separate, blocked channel. *See Denver Area Ed. Tel. Consort. v FCC,* 116 S. Ct. 2374 (1996). *See also Playboy Entertainment Group v United States,* 945 F. Supp. 772 (D. Del. 1996), *aff'd,* 117 S. Ct. 1309 (1997) (upholding CDA's cable indecency provisions).

computer "Internet" indecency—The Communications Decency Act of 1996 ("CDA"), 110 Stat. 133-43, amended 47 U.S.C. § 223 to add a new subsection 223 (d) to prohibit knowingly sending or displaying "indecent" material to minors under age 18 by computer and defined the indecency which is unlawful to provide to minors as: *"any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." See Joint Explanatory Statement of the Committee of Conference* ("Conference Report on the CDA"), 1996 U.S.C.C.A.N. Leg. Hist., at 200-11. The indecency provisions for interactive computer systems were held unenforceable in *Reno v ACLU,* 117 S. Ct. 2329 (1997), but the Court reaffirmed the application of obscenity and child pornography laws in "cyberspace."

pornography—A generic term that can refer to materials that are either "legal" or "illegal" to disseminate under the circumstances. "Pornography" encompasses all sexually oriented material intended primarily to arouse the reader, viewer, or listener. *See Webster's Dictionary; Miller v California,* 413 U.S. 15, 18 n. 2 (1973); *Final Report,* Attorney General's Commission on Pornography (1986), Chapter One, "Defining our Central Terms." Serious works of art, literature, politics, or science; "mere nudity," medical works, even though they deal with sex or include sexual references or depictions, would not be considered "pornography" in the context of their legitimate uses. On the other hand, since obscenity can include both actual and simulated conduct, all "Hard-Core Pornography" that depicts penetration clearly visible ("PCV") is "implicitly" within the application of the constitutional criteria of the Supreme Court's obscenity test. *See Mishkin v New York,* 383 U.S. 506, 508 (1966), *Miller v California,* 413 U.S. 15, 29 (1973).

Legal definitions from National Law Center for Children and Families, 4103 Chain Bridge Rd. #410, Fairfax, VA 22030-4105, 703-691-4626, fax: 703-691-4669. Used by permission.

End of Comment